FIGHT FOR THE FUTURE
EDUCATION FUND

December 6, 2017

EX PARTE WRITTEN SUBMISSION

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

Re: *Restoring Internet Freedom*, WC Docket No. 17-108

Dear Ms. Dortch:

We write today to raise concerns regarding the inability of the Federal Communications Commission ("FCC" or "Commission") to maintain a functioning electronic comment system in the *Restoring Internet Freedom* proceeding. As a result of alleged distributed denial-of-service attacks on the Commission's website and the submission of potentially millions of fraudulent comments in the docket, we have serious questions about the transparency of the rulemaking process, the legitimacy and fairness of the proceeding, and whether the public has been able to have their voices heard, as is required under the Administrative Procedure Act.

DDoS Attacks

Overview

For a rulemaking, the FCC must comply with the notice and comment requirements of the Administrative Procedure Act (the "APA"). The APA requires that the FCC "give interested persons an opportunity to participate in the rule making through the submission of written data, views or arguments."[1] This requirement is not met when technical and administrative burdens prevent the public from participating in the rulemaking process. Thus, any rules promulgated following an inadequate process are arbitrary and capricious and in violation of the APA.

For several periods of time during the public comment period in the *Restoring Internet Freedom* proceeding, the FCC's electronic comment system was unavailable and commenters could not file comments with the FCC. The technical failures experienced on the FCC website deprived the public of the ability to participate in the rulemaking. As a result, the net neutrality rulemaking

[1] 5 U.S.C. § 553. *See, e.g., Home Box Office, Inc. v. FCC, 567 F.2d 9,34 (D.C. Cir. 1977)* (vacating final rule due to the FCC's failure to comply with the notice and comment requirements of the Administrative Procedure Act "that are intended to …provide fair treatment for persons affected by a rule." The Court noted that "an agency must comply with the procedures set out in Section 4 of the APA." (quoting *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 407 (1971)); *Am. Radio Relay League, Inc. v. FCC*, 524 F.3d 227 (D.C. Cir. 2008) (remanding final rule based on a finding that the FCC failed to comply with the Administrative Procedure Act).

failed to meet the requirements of the APA and any rules promulgated from the rulemaking would be arbitrary and capricious and in violation of the APA.

Additionally, questions about the FCC's network security and its investigation into alleged distributed denial-of-service (DDoS) attacks have raised concerns regarding issues of transparency and the legitimacy and fairness of the proceeding. Following a joint press conference with New York Attorney General Eric Schneiderman, even one of the FCC's own Commissioners sounded the alarm bells over the lack of integrity in the FCC process.[2]

While the FCC reports that multiple DDoS attacks occurred around midnight on May 7-8, 2017, they later stated that there is no written documentation to support this conclusion. The FCC refuses to release its logs for review by an independent security analyst. It is unclear if and/or when the Commission notified the FCC's Office of Inspector General, Congress (as required by the Federal Information Security Management Act), or the National Cybersecurity and Communications Integration Center's Hunt and Incidence Response Team of these attacks. The Government Accountability Office is investigating whether these alleged DDoS attacks even occurred and if they occurred, whether the FCC took adequate measures to address the attacks.

Given the information we have at this point, we believe that it is likely that no such DDoS attacks occurred but rather, the FCC was unprepared to handle high amounts of traffic, and as a result, experienced system difficulties, leading to individuals not being able to comment on the proceeding.

Timeline of Events

In a press release dated May 8, 2017, FCC Chief Information Officer Dr. David Bray reported that the FCC website experienced multiple DDoS attacks around midnight on May 7-8, 2017.[3] He stated that the attacks were "deliberate attempts by external actors to bombard the FCC's comment system with a high amount of traffic to [its] commercial cloud host."[4] Even though the comment system remained running, legitimate commenters could not access and file comments with the FCC.

The timing of the DDoS attacks is suspicious as the attacks occurred around the same time as comedian John Oliver's show "Last Week Tonight." On his show, Oliver aired a segment on net neutrality and directed his viewers to the FCC's website to submit comments in support of the current net neutrality rules. Despite multiple media reports that the FCC website server problems were a result of being bombarded by a high amount of traffic from Oliver's show,[5] the FCC

---

[2] Press Release, Federal Communications Commission, Statement of Commissioner Jessica Rosenworcel on Lack of Integrity in FCC Process (December 4, 2017), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db1204/DOC-348056A1.pdf.

[3] Press Release, Federal Communications Commission, FCC CIO Statement on Distributed Denial-of-Service Attacks on FCC Electronic Comment Filing System (May 8, 2017), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-344764A1.pdf.

[4] *Id.*

[5] Sam Gustin, *John Oliver Just Crashed the FCC's Website Over Net Neutrality- Again,* MOTHERBOARD (May 8, 2017, 8:25am),

maintains that the cause of the server problems was multiple DDoS attacks. Multiple requests for documentation related to the attacks have been made to the FCC, but to date, the FCC has declined to provide any proof that the DDoS attacks actually occurred. A high influx of requests and comments could easily be mistaken for a DDoS attack.[6] In 2014, the FCC suffered similar problems with its website when John Oliver aired his first segment on net neutrality.[7] In 2014, the FCC's security team internally assessed that there was no evidence of a malicious intrusion in relation to the server problems.[8]

In addition to the FCC electronic comment system being unavailable during the DDoS attacks on May 7-8, 2017, the FCC servers were down and commenters were not able to access the FCC electronic comment system at multiple other times. Even prior to the first airing of the John Oliver segment on May 7, 2017, FCC employees acknowledged in emails to us that the FCC was having "server issues."[9] When Oliver's segment re-aired on Monday, May 8, 2017 at 8:30pm EST, again, the FCC servers went down around the time of the program. Screenshots showing the server errors are attached as Appendix A.

On May 9, 2017, in response to the FCC's press release, Senators Ron Wyden and Brian Schatz sent a letter to Chairman Pai inquiring about the DDoS attacks. In the letter, the Senators asked a series of questions about the attacks and requested that the FCC make available alternative ways for the public to comment on the proceeding, such as a dedicated email account for the net neutrality proceeding as was done in 2014. The Chairman responded to the Senators in a letter on June 15, 2017. The May 9th letter from the Senators and the response from the Chairman are attached as Appendix B. While the Chairman cited the record number of comments the Commission had received, he was unable to cite how many individuals had been prevented from participating in the rulemaking due to the problems with the FCC electronic comment system. Additionally, the Chairman indicated that the attacks appeared to be "cloud-based."[10] If this is indeed the case, cloud providers keep records of the exact resources used by each account for billing purposes. It is unclear why the FCC has not taken available legal steps to obtain these

---

https://motherboard.vice.com/en_us/article/3dxdqb/john-oliver-just-crashed-the-fccs-website-over-net-neutralityagain. *See also* Jeff John Roberts, *John Oliver Gets Fired Up Over Net Neutrality-and FCC's Site Goes Down,* FORTUNE (May 8, 2017), http://fortune.com/2017/05/08/john-oliver-net-neutrality/.

[6] *FCC Filings Overwhelmingly Support Net Neutrality Once Anti-Net Neutrality Spam is Removed*, JFoss Blog (May 13, 2017), http://jeffreyfossett.com/2017/05/13/fcc-filings.html.

[7] Soraya Nadia McDonald, *John Oliver's net neutrality rant may have caused FCC site crash*, THE WASHINGTON POST (June 4, 2014), https://www.washingtonpost.com/news/morning-mix/wp/2014/06/04/john-olivers-net-neutrality-rant-may-have-caused-fcc-site-crash/?utm_term=.a510e8afd2f2. *See also* Dell Cameron, *Senior US Official Claimed the FCC Got "Hacked" After Security Professionals Found no Proof,* GIZMODO (August 7, 2017, 12:20pm), https://gizmodo.com/senior-us-official-claimed-the-fcc-got-hacked-after-sec-1797593781.

[8] Cameron, *supra* note 7.

[9] Fight for the Future, *What is the FCC hiding? Thousands call for the agency to provide evidence of alleged DDoS attacks that silenced net neutrality supporters,* FIGHT FOR THE FUTURE (May 11, 2017, 7:39pm), https://www.fightforthefuture.org/news/2017-05-11-what-is-the-fcc-hiding-thousands-call-for-the/.

[10] Letter from Ajit Pai, Chairman, Federal Communications Commission, to Honorable Ron Wyden, United States Senate (June 15, 2017), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-345556A1.pdf. Letter from Ajit Pai, Chairman, Federal Communications Commission, to Honorable Brian Schatz, United States Senate (June 15, 2017), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-345556A1.pdf.

records and determine who attacked the FCC system. It is the responsibility of the FCC to employ basic cybersecurity practices that prevent abuse and outages, including the ability to block malicious traffic by IP addresses, and simple scaling strategies, like caching slow database queries.

On July 7, 2017, Senators Ron Wyden and Brian Schatz sent a follow-up letter to Chairman Pai, Commissioner Clyburn and Commissioner O'Rielly to express concerns with the FCC cybersecurity preparedness and multiple reported problems with the FCC's website in taking public comments in the *Restoring Internet Freedom* proceeding. The Chairman replied to the Senators in a letter on July 11, 2017. The July 7th letter from the Senators and the response from the Chairman are attached as Appendix C. In the reply letter, the Chairman failed to respond to the Senators' questions. Instead, he informed the Senators that the FCC's plans to secure the system must remain secret in order not to "undermine our system's security."[11]

On May 21, 2017, the Gizmodo Media Group submitted a Freedom of Information Act ('FOIA") Request to the FCC for information and documentation related to the DDoS attacks. In response to the FOIA Request, attached hereto as Appendix D, the FCC confirmed that "there are no records" related to the FCC analysis that concluded DDoS attacks had taken place.[12] The FCC's analysis "stemmed from real time observation and feedback from Commission IT staff and did not result in written documentation."[13] In total, only 16 pages were released to Gizmodo, many of which were fully redacted.[14] The FCC refused to release 209 pages related to the DDoS attacks based on varying justifications.[15]

Due to continued unanswered questions and the unwillingness of the FCC to provide any requested documentation, on August 17, 2017, Senator Brian Schatz and Representative Frank Pallone sent a letter, attached hereto as Appendix E, to the Comptroller of the United States, requesting that the Government Accountability Office investigate the attacks. The Congressmen raised concerns that the FCC had not released any documentation confirming that the DDoS attacks had actually occurred, that if such attacks had occurred, whether the attacks were effectively addressed, and whether the FCC had taken measures to thwart future attacks and secure its systems. In October 2017, the Government Accountability Office ("GAO") confirmed that it will investigate the alleged attacks.[16] Charles Young, a spokesman for GAO, stated that the

---

[11] Letter from Ajit Pai, Chairman, Federal Communications Commission, to Honorable Ron Wyden, United States Senate (July 11, 2017), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-345883A1.pdf. Letter from Ajit Pai, Chairman, Federal Communications Commission, to Honorable Brian Schatz, United States Senate (July 11, 2017), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-345883A1.pdf.

[12] Letter from Elizabeth Lyle, Assistant General Counsel, Federal Communications Commission, to Dell Cameron, Gizmodo Media Group (July 19, 2017), *available at* https://drive.google.com/file/d/0B843Xk5ioULqODFCME1OemdKZ0U/view.

[13] *Id.*

[14] Dell Cameron, *FCC Now Says There is No Documented 'Analysis' of the Cyberattack it Claims Crippled its Website in May,* GIZMODO (July 19, 2017, 9:35pm), https://gizmodo.com/fcc-now-says-there-is-no-documented-analysis-of-the-cyb-1797073113.

[15] *Id.*

[16] Jon Brodkin, *FCC's DDoS claims will be investigated by government,* ARSTECHNICA (Oct. 16, 2017, 4:25pm), https://arstechnica.com/tech-policy/2017/10/fccs-ddos-claims-will-be-investigated-by-government/.

office would be investigating the service interruption, missing emails, and automated comments using people's identities without their knowledge.[17] The investigation, however, will not begin for several months, likely after the FCC votes on the final order.[18]

Conclusion

Given the unavailability of the FCC electronic comment system for multiple periods of time during the *Restoring Internet Freedom* proceeding, the FCC has failed to comply with the requirements of the APA to give the public an opportunity to comment.[19] As a result of failing to comply with the APA, any rules promulgated following this inadequate process, would be arbitrary and capricious and in violation of the APA. Moreover, the legitimacy and fairness of the FCC's process is further undermined by the FCC's failure to provide any documentation, including in response to multiple requests from Congressmen and Freedom of Information Act Requests, as to whether the alleged DDoS attacks even occurred. It is our continued belief that the DDoS attacks did not occur and the website problems were the result of an inadequate system that could not handle a high amount of traffic, as was the case in 2014 when the FCC experienced similar problems following a John Oliver segment on net neutrality.

Fraudulent Comments

Overview

The APA requires that the final rules in a rulemaking be based on the record before the Commission.[20] If the record before the Commission is tainted or if the Commission bases its final rule on fake comments, the Commission will have acted in an arbitrary and capricious manner, in violation of the APA. In order to meet the "arbitrary and capricious" standard, the Commission must "examine the relevant data and articulate a satisfactory explanation for its action including a 'rational connection between the facts found and the choice made.'"[21] If the Commission does not investigate and address the anomalies in the record, it will not be able to meet the standard in this rulemaking.

In the *Restoring Internet Freedom* proceeding, there have been numerous reports by citizens, experts, media outlets and advocacy organizations such as ours that at least one million comments, if not more, have been fraudulently submitted in the docket, both using stolen names

[17] Todd Shields, *FCC Got 444,938 Net-Neutrality Comments from Russian Email Addresses,* BLOOMBERG POLITICS (Nov. 29, 2017, 11:05am), https://www.bloomberg.com/news/articles/2017-11-29/fake-views-444-938-russian-emails-among-suspect-comments-to-fcc.

[18] Brodkin, *supra* note 16.

[19] 5 U.S.C. § 553.

[20] 5 U.S.C. § 553. *See* also Office of the Federal Register, A Guide to the Rule Making Process 5-6 (2017) (noting that "the agency must base its reasoning and conclusions on the rulemaking record, consisting of the comments, scientific data, expert opinions, and facts accumulated during the pre-rule and proposed rule stages."), available at https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.

[21] *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co*., 463 U.S. 29, 43 (quoting *Burlington Truck Lines, Inc. v. United States*, 371 U.S. 156, 168 (1962)).

and addresses and made-up names and addresses. Despite acknowledging the widespread irregularities in the record,[22] the FCC failed to launch an investigation, to take measures to prevent further harm to individuals or to ensure that the public comment process remained open to the public as legally required. As a result of the FCC's willful inaction, the legitimacy and fairness of the proceeding have been comprised. Serious questions have been raised as to whether federal law has been violated and whether parties may be attempting to influence federal policy by misrepresenting the views of innocent victims.

Timeline of Events

Reports first began to surface in May 2017 that the docket contained fraudulent anti-net neutrality comments.[23] The most recent reports, including reports by the New York Attorney General and Commissioner Rosenworcel, estimate that over one million comments have been fraudulently submitted in the docket using stolen names and addresses.[24] There have also been reports that comments are missing from the docket.[25] Estimates and claims from these reports are as follows:

- Fox 31 Denver reported that more than 7,000 Coloradans' names and addresses have been used to post fake comments in the net neutrality docket.[26]

---

[22] Dell Cameron, *FCC Internal Watchdog Agrees to Aid Probe of Fake Net Neutrality Comments*, GIZMODO (Dec. 4, 2017, 4:07pm), https://gizmodo.com/fcc-s-internal-watchdog-agrees-to-help-new-york-s-probe-1820987362*;* Todd Shields, *FCC Got 444,938 Net-Neutrality Comments from Russian Email Addresses,* BLOOMBERG POLITICS (Nov. 29, 2017, 11:05am), https://www.bloomberg.com/news/articles/2017-11-29/fake-views-444-938-russian-emails-among-suspect-comments-to-fcc (Brian Hart, FCC spokesman, acknowledged the "concerning activity" in the record.); Kevin Collier, *FCC is Honoring Fake Anti-Net Neutrality Rants Left By Bots,* VOCATIVE (May 18, 2017, 3:42pm), http://www.vocativ.com/431065/fcc-ajit-pai-net-neutrality-bots/.

[23] Press Release, Fight for the Future, *The FCC cannot move forward until it investigates flood of anti-net neutrality comments using stolen names and addresses* (May 17, 2017), https://www.fightforthefuture.org/news/2017-05-17-the-fcc-cannot-move-forward-until-it-investigates/. *See also* Dominic Rusche, *'Pretty ridiculous': thousands of names stolen to attack net neutrality rules*, THE GUARDIAN (May 26, 2017), https://www.theguardian.com/technology/2017/may/26/fcc-net-neutrality-open-internet.

[24] Hamza Shaban, *FCC commissioner, New York attorney general call for delay of net neutrality vote over fake comments*, THE WASHINGTON POST (Dec. 4, 2017, 4:46pm), https://www.washingtonpost.com/news/the-switch/wp/2017/12/04/fcc-commissioner-new-york-attorney-general-call-for-delay-of-net-neutrality-vote-over-fake-comments/?utm_term=.75debfb80033; Nikhil Sonnad, *How a bot made 1 million comments against net neutrality look genuine,* QUARTZ (Nov. 28, 2017), https://qz.com/1138697/net-neutrality-a-spambot-made-over-a-million-anti-net-neutrality-comments-to-the-fcc/.

[25] Letter from Frank Pallone, Jr. and Elijah E. Cummings, Members, U.S. House of Representatives, to Chairman Ajit Pai, Commissioner Mignon Clyburn and Commissioner Michael O'Rielly, Federal Communications Commission (June 26, 2017), *available at* https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/FCC.Chairman.Commissioners.2017.06.26.%20Letter%20to%20FCC%20re%20cybersecurity%20prepardness%20and%20public%20comments.CAT_.OI%5B1%5D.pdf.

[26] Emily Allen, *7,000-plus Coloradans' names, addresses used to post fake comments about government decision,* FOX 31 DENVER (May 14, 2017, 9:51pm), http://kdvr.com/2017/05/14/7000-coloradans-names-addresses-used-to-post-fake-comments-about-government-decision/.

- In May 2017, ZdNet reported that more than 128,000 anti-net neutrality comments were identical, with the spambot leaving the comments in alphabetical order with the person's name, postal address and zip code.[27] There is speculation that the spambot obtained the information from public voter registration records or an older data breach. Multiple news outlets contacted individuals who supposedly posted comments only to be told by individuals that they did not write the comments and they did not know where the comments came from or even that deceased individuals were submitting comments.[28]
- At its peak, the anti-net neutrality spambot campaigns produced tens of thousands of identical comments. These comments were all formatted consistently and designed to look like real submissions.[29] During one 24-hour period, anti-net neutrality spambot campaigns produced roughly 17,000 identical comments.[30]
- In May 2017, The Verge reported that a high percentage of personal information used by the anti-net neutrality bot spamming the FCC overlapped with information in data breaches.[31] This was confirmed by independent data analysis.[32] One analysis of a random sampling of 1,000 comments found that approximately 76% of emails associated with repeated comments had been involved in one data breach and approximately 66% were part of the River City Media data breach.[33]
- As of November 29, 2017, 444,938 comments were filed from Russian email addresses.[34] It is unclear whether these were from Russian citizens or from bots.
- As of November 23, 2017, an analysis by a data scientist using natural language processing techniques revealed that one anti-net neutrality spam campaign used mail

---

[27] Zack Whittaker, *Anti-net neutrality spammers are flodding FCC's pages with fake comments,* ZDNET (May 10, 2017, 10:32am), http://www.zdnet.com/article/a-bot-is-flooding-the-fccs-website-with-fake-anti-net-neutrality-comments/.

[28] Colin Lecher, Adi Robertson and Russell Brandon, *Anti-net neutrality spammers are impersonating real people to flood FCC comments,* THE VERGE (May 10, 2017, 11:16am), https://www.theverge.com/2017/5/10/15610744/anti-net-neutrality-fake-comments-identities; Zack Whittaker, *Anti-net neutrality spammers are flodding FCC's pages with fake comments,* ZDNET (May 10, 2017, 10:32am), http://www.zdnet.com/article/a-bot-is-flooding-the-fccs-website-with-fake-anti-net-neutrality-comments/; Fight for the Future, *The FCC cannot move forward until it investigates flood of anti-net neutrality comments using stolen names and addresses,* FIGHT FOR THE FUTURE (May 17, 2017, 12:28pm), https://www.fightforthefuture.org/news/2017-05-17-the-fcc-cannot-move-forward-until-it-investigates/; James Harvey, *Ajit Pai's FCC Looking at False Public Comments*, MEDIUM (Oct. 26, 2017), https://medium.com/@vajrajames/ajit-pais-fcc-looking-at-false-public-comments-c5c82a72d22 (Author documents how he knocked on doors and recorded conversations in his home town, the vast majority of people he talked with did not submit comments. He found comments submit by a deceased individual and associated with addresses where people had not lived for long periods of time).

[29] Chris Sinchok, *An Analysis of the Anti-Title II bots,* MEDIUM (May 14, 2017), https://medium.com/@csinchok/an-analysis-of-the-anti-title-ii-bots-463f184829bc.

[30] Colin Lecher, Russell Brandon and Adi Robertson, *The anti-net neutrality bot spamming the FCC is pulling names from leaked databases,* THE VERGE (May 11, 2017, 3:44pm), https://www.theverge.com/2017/5/11/15626278/net-neutrality-spam-bot-fcc-leak-data.

[31] *Id.*

[32] Sinchok, *supra* note 29.

[33] *FCC Filings Overwhelmingly Support Net Neutrality Once Anti-Net Neutrality Spam is Removed*, JFoss Blog (May 13, 2017), http://jeffreyfossett.com/2017/05/13/fcc-filings.html.

[34] Shields, *supra* note 17.

merge to disguise 1.3 million comments as unique grassroot submissions.[35] There were likely multiple spambots used to file comments in the proceeding in a similar manner.

- Data scientist Jeff Kao explained how every one of the 1.3 million anti-net neutrality comments had the same structure as below, with each of the terms in brackets chosen to create unique combinations. The structure appeared as follows:
  - Dear [FCC]. I strongly [urge/recommend/ask] the FCC to [rescind/overturn/undo] the rules [set in place/laid down] by [Obama/Wheeler/both], which [take over broadband/control the internet]. [Normal people], as opposed to [elitist liberal bureaucrats], should be able to [use/purchase] the [services/applications/products] they want. The [Obama/Wheeler/both] plan is a [betrayal/exploitation/corruption] of [net neutrality/the open internet]. It [undid/reversed/broke] a [light-touch/market-based/pro-consumer] [approach/policy/system] that [worked/functioned/performed] successfully for [a long time] with [bipartisan support].[36]

In response to these numerous reports of identity theft, in May 2017, we launched a website, www.Comcastroturf.com, to allow individuals to check to see if their names or personal information were used to file a comment with the FCC without their permission and to assist those who had been victims of identity theft to contact authorities to request an investigation. We received a number of verified reports of people whose identities had been stolen and used to submit comments without their permission. Additionally, as of December 6, 2017, over 2,400 people used the website to contact their State Attorney Generals.[37]

On May 25, 2017, a group of 27 individuals sent a letter to Chairman Pai and Dr. David Bray, attached hereto as Appendix F, informing the Chairman that the individuals' names and personal information were used to file comments in the docket that they did not make. In the letter, they requested the Chairman take the following actions: (i) notify all who had been impacted by the attack; (ii) remove all fraudulent comments from the docket immediately, including the comments that they identified as being fraudulently made in their names, (iii) publicly disclose any information that the FCC had as to the party or parties responsible for the fraudulent comments, and (iv) call for an investigation by the appropriate authorities into possible violations of 18 U.S.C. §1001 and other relevant laws. The FCC failed to take any actions in response to

---

[35] Jeff Kao, *More than a Million Pro-Repeal Net Neutrality Comments Were Likely Faked*, HACKERNOON (Nov. 23, 2017), https://hackernoon.com/more-than-a-million-pro-repeal-net-neutrality-comments-were-likely-faked-e9f0e3ed36a6?curator=MediaREDEF. *See also* Nikhil Sonnad, *How a bot made 1 million comments against net neutrality look genuine,* QUARTZ (Nov. 28, 2017), https://qz.com/1138697/net-neutrality-a-spambot-made-over-a-million-anti-net-neutrality-comments-to-the-fcc/.

[36] Sonnad, *supra* note 35.

[37] Fight for the Future, *Victims whose stolen names and addresses were used to submit fake anti-net neutrality comments send letter to FCC demanding investigation*, FIGHT FOR THE FUTURE (May 25, 2017, 10:54am), https://www.fightforthefuture.org/news/2017-05-25-victims-whose-stolen-names-and-addresses-were-used/.

being notified that these 27 individuals' names and personal information had been stolen and continued to be displayed on the FCC website without their permission.

Representative Frank Pallone has also expressed alarm as to whether federal law has been violated by fake comments being submitted to the FCC using stolen names and personal information. On June 28, 2017, he sent a letter, attached hereto as Appendix G, to the FBI and Department of Justice, urging them to investigate whether there was a coordinated attack to violate federal law.

For the last six months, the New York Attorney General Eric Schneiderman has also been investigating who is behind this massive scheme to steal New Yorkers' identities and file fraudulent comments. The New York Attorney General's Office has analyzed the fake comments and determined that tens of thousands of New Yorkers have had their identities misused.[38] The New York Attorney General's Office has also determined that tens of thousands of Americans in each of California, Georgia, Missouri, Ohio, Pennsylvania and Texas have had their identities misused.[39] Only after nine requests to the FCC for logs and other records to aid in a law enforcement investigation to determine who is misusing people's identities and a press conference has the FCC finally agreed on December 4, 2017 to assist with the investigation.

Moreover, the mere widespread reporting on the fake comments and the fact that the FCC was actively choosing not to take any measures to stop these malicious actors from corrupting the public record, in and of itself inhibited participation in the public comment process in the *Restoring Internet Freedom* proceeding. Many individuals rightly got the impression that the public comment process was tainted—or that if they participated their data could be misused by malicious actors—and were discouraged from participating. The chilling effect of the FCC's inaction on the public comment process cannot be overstated. The FCC took no action, despite having knowledge that federal law against making false statements in a federal proceeding had been broken potentially millions of times. The FCC had obvious avenues of mitigation and investigation, such as blocking IP addresses associated with fake addresses, making public the IP addresses used for known fake comments, obtaining the billing information for the cloud services used, or at the very minimum, involving the appropriate federal authorities to investigate these reports, but instead, the FCC did nothing. The FCC only agreed to assist with New York State's investigation into the fake comments after repeated requests for six months.

Federal law guarantees every American a voice in the process. People should not be discouraged from participating in the process because they are afraid their personal information will be stolen. Numerous individuals told us that they did not submit comments for this reason. Other individuals expressed concern over the FCC making their email address public through the API. Using the email addresses from the API, spammers could have downloaded legitimate comments and resubmitted them with identical information or harassed individuals, stifling legitimate participation. Additionally, if one's personal information was stolen, the FCC made it clear through their inaction that an individual had no recourse. While one news outlet reported that the

[38] Eric Schneiderman, *An Open Letter to the FCC*, MEDIUM (Nov. 21, 2017), https://medium.com/@AGSchneiderman/an-open-letter-to-the-fcc-b867a763850a.
[39] *Id.*

FCC was encouraging individuals who found comments falsely posted in their name to submit their actual comment and information about the false comment,[40] there does not appear to be an official statement from the FCC as to how fake comments should be handled. Additionally, this guidance does nothing to remove the stolen personal information or protect the individual from further harm. It does not remedy the violation that an individual feels when they find their name signed to a belief that has been made public and is not theirs.

Conclusion

Widespread irregularities in the record for the *Restoring Internet Freedom* proceeding have been reported by citizens, experts, media outlets and advocacy organizations. Millions of comments may have been fraudulently submitted using stolen names. Despite acknowledging that the electronic comment system is susceptible to abuse and that comments have been submitted into the record using both stolen and made-up names and personal information, the FCC has failed to launch an investigation, to take measures to stop the fraudulent practice, or to address the underlying problem. Furthermore, the FCC's unwillingness to stop malicious actors from corrupting the public record and to investigate repeated violations of federal law has had a chilling effect and discouraged people from participating in the public comment process for fear that their personal information will be stolen and that the process has been tainted. If the Commission bases its final rule on a tainted record, and a process that inhibited participation by the public, it will have acted in an arbitrary and capricious manner, in violation of the APA.

Sincerely,

/Holmes Wilson/
Holmes Wilson
Co-Director
Fight for the Future
PO Box 55071 #95005
Boston, MA 02205

[40] Edward C. Baig and Elizabeth Weise, *Millions of net neutrality comments were faked. Turns out mine was one.,* USA TODAY (Dec. 6, 2017, 6:00am), https://www.usatoday.com/story/tech/2017/12/06/fake-names-and-c-used-fcc-internet-regulation-debate-public-comments-includes-usa-today-tech-columni/923576001/.